**AFFIDAVIT IN SUPPORT OF**
**AN APPLICATION FOR A SEARCH WARRANT**

I, Edgar Jones, being duly sworn, hereby depose and state as follows:

1. This affidavit is made in support of an application for a warrant to search an unlocked black Samsung Galaxy S23 smartphone, IMEI # 351997884440811, seized as an evidentiary item following the arrest of its owner, hereinafter referred to as the TARGET TELEPHONE, as described more fully in Attachment A, for violations of Section 1546(a) of Title 18, United States Code. TARGET TELEPHONE belongs to Carlos FIGUEROA, a previously removed Honduran national.

2. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1546(a) Visa Fraud, as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

3. I am a Special Agent (SA) with the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) and have been since October of 2009. Prior to ICE HSI's creation, between 2007 and 2009, I served as an Immigration Enforcement Agent with the Enforcement and Removal Operations (ERO) component of ICE. I attended the Federal Law Enforcement Training Center at Glynco, Georgia. I completed the ICE Academy, which included training in enforcing Title 8 of the United States Code. I subsequently graduated from the Criminal Investigator Training Program, which included training in investigating violations of Title 18 of the United States Code. I have a combined total of over 17 years of conducting immigration-related investigations, which led to successful prosecutions of violators of Titles 8 and 18 of the United States Code. I serve as

a liaison to ERO as needed and have previously investigated and prosecuted subjects engaged in document fraud.

4. Based upon my training and my law enforcement experience, I know: (a) Subjects who purchase or sell fraudulent identification documents very often use cellular devices and computers to communicate with co-conspirators; (b) Subjects trafficking fraudulent ID documents use cellular devices and computer memory both internal and external to store information including but not limited to ledgers, names, emails, recent and past banking information, illegally obtained items of value; and (c) Subjects trafficking fraudulent IDs very often use various cellular devices and computers to track locations of their activities.

5. The facts set forth in this affidavit are based upon information known to me personally from this investigation, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant and does not purport to set forth all my knowledge of the investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

## PROBABLE CAUSE

6. On September 26, 2024, the Overland Park, Kansas Police Department (OPPD) briefed HSI Kansas City on Carlos FIGUEROA, date of birth 11/07/1986, a suspected manufacturer of fraudulent identification documents operating out of 9340 Mackey Street, Overland Park, Kansas. OPPD Detective Joshua Raniag said that a tipster had advised their agency that FIGUEROA operated printers at night to produce fraudulent Lawful Permanent Resident cards, which he distributed during the day.

7. Immigration databases revealed that FIGUEROA was previously deported to Honduras on July 4, 2014. HSI Kansas City reviewed the contents of the alien file of FIGUEROA and confirmed that he did not have special permission to re-enter the United States. Law enforcement databases revealed that FIGUEROA obtained an authentic Colorado driver's license on October 12, 2023, which listed his address as 1135 Swift Gulch Rd, Apt. 12-204, Avon, Colorado, 81620.


Removal photo of FIGUEROA CO DL # 172378514

8. Customs databases revealed that on October 23, 2023, United States Customs and Border Protection (CBP) conducted a border search of an inbound package from Hong Kong en route to FIGUEROA at 9340 Mackey Street, Overland Park, Kansas. It was manifested as a wallet, but the wallet was found to contain two identical counterfeit Kansas driver's licenses displaying the name, date of birth, photo, and prior operator license number of FIGUEROA: FIGUEROA previously obtained a State of Kansas DL due to having been issued employment authorization by DHS. CBP seized the package and turned it over to their Fraudulent Document Analysis Unit. I subsequently requested the evidence and delivered the counterfeit Kansas DLs to the Kansas Department of Revenue.





9. ERO Kansas City officers conducted surveillance of 9340 Mackey Street, in Overland Park beginning in April of 2024, but did not observe FIGUEROA there.

10. The Kansas Department of Revenue advised that FIGUEROA applied for and obtained a Kansas title for a 2023 Chevrolet Silverado which he bought on July 23, 2024, in Texas for a total sale price of $40,000 (trade-in valued at $39,000). On the state inspection form, FIGUEROA listed his Colorado driver's license number and provided his address as 9340 Mackey Street, Overland Park, Kansas. There is no recorded lien on this vehicle.

11. The Kansas Department of Labor subsequently advised that the last known employment of FIGUEROA reported by an employer was in the fourth quarter of 2014 in Kansas City, Kansas. The Missouri Department of Labor advised that the last known Missouri employment of FIGUEROA was in the second quarter of 2014.

12. On the morning of September 27, 2024, OPPD detectives observed FIGUEROA and a female Hispanic subject removing large black trash bags that appeared to be full of items from 9340 Mackey Street into their vehicles, the 2023 Chevrolet Silverado and a red Alfa Romeo Stelvio crossover style sport-utility vehicle. The Alfa Romeo is also titled and registered to FIGUEROA. FIGUEROA and the female subject then drove to 10914 W. 71st Street in Shawnee, Kansas. They unloaded the large black trash bags and brought them into the house.

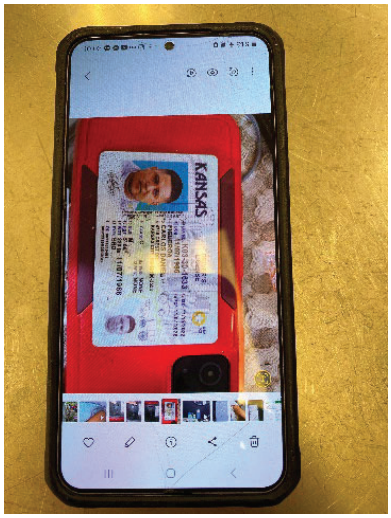
13. The Alfa Romeo displayed Kansas temporary license plate ABHR2 and an expiration date of November 16, 2024. Kansas temporary license plates are generally valid for 60 days from purchase, which indicates this vehicle was bought on or about September 16, 2024. The Kansas Department of Revenue advised that no title or license plate application has been received yet, and there is no known lien on this vehicle.

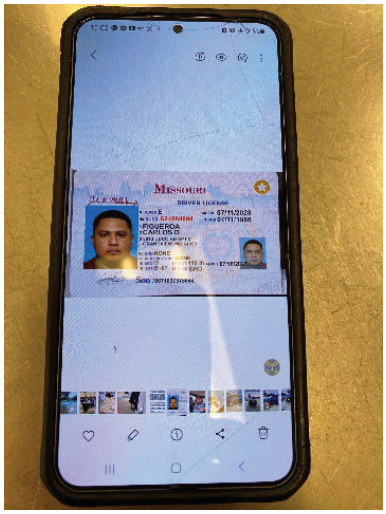
14. On the morning of October 7, 2024, HSI Special Agent Michael Sweetin and I conducted surveillance of the suspected new address of Carlos FIGUEROA at 10914 W 71st Street in Shawnee, KS. FIGUEROA's Chevrolet Silverado was parked in the driveway, and a male Hispanic subject whose physical appearance was consistent with FIGUEROA exited the house after a garbage truck arrived and left. Consequently, it appeared that FIGUEROA had moved to 10914 W 71st Street in Shawnee, Kansas.

15. On the morning of October 29, 2024, ERO Kansas City officers conducted mobile surveillance of FIGUEROA as he traveled to Overland Park, Kansas. At approximately 0900 hours, ERO administratively arrested FIGUEROA for illegal re-entry by a removed alien, pursuant to section 212(a)(9)(A)(ii) of the Immigration and Nationality Act, Alien Previously Removed. S/A Sweetin and I then traveled to ERO Kansas City, 11125 N. Ambassador Drive, Suite 100, Kansas City, Missouri, 64153.

16. S/A Sweetin and I identified ourselves to FIGUEROA using our department-issued credentials, and FIGUEROA claimed that his English was very limited. FIGUEROA requested Spanish assistance via telephone from his daughter, Daniela Getsemani FIGUEROA-Cardona, (816) 681-8885. At approximately 0939 hours, FIGUEROA consented, both verbally and in writing for HSI to search his black Samsung smartphone.

17. On his phone, I located photos of fraudulent Kansas and Missouri driver's licenses displaying photos of FIGUEROA and his identifiers. The photo of the counterfeit Kansas DL was identical to the counterfeit Kansas DLs previously seized by CBP.

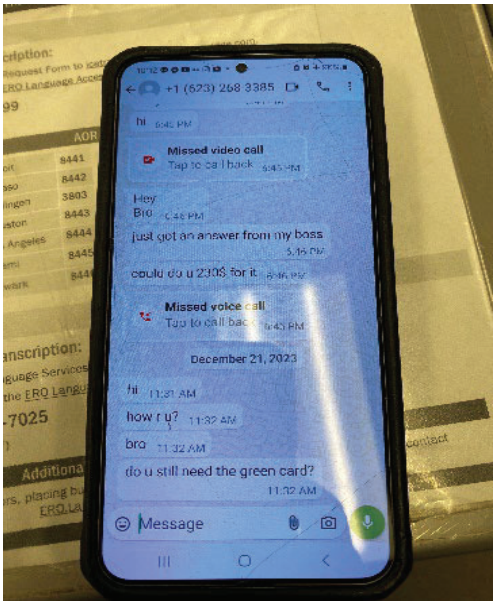



18. FIGUEROA displayed to S/A Sweetin and me several WhatsApp messages regarding the purchase of a fraudulent Lawful Permanent Resident card. The last page of the messages from telephone number (623) 268-3385 read as follows:

(Unknown date prior to December 21, 2023) "hi Hey Bro just got an answer from my boss could you do 230$ for it"

(December 21, 2023) "hi how r u? bro do u you still need the green card?"




19. Although it appears that the WhatsApp messaging was regarding a potential purchase of a fraudulent Lawful Permanent Resident card by FIGUEROA, it's possible that he may have obtained this variety of fraudulent identification documents to use them as templates to manufacture these types of fraudulent ID documents.

20. FIGUEROA also displayed to me a video of a female subject he identified as his wife Carmen firing a black semi-automatic pistol. Immigration databases showed that Carmen Sarahy FIGUEROA-Lopez has been assigned alien file A205755618. Although her deportation proceedings were terminated and she was issued a work card, she does not currently have any lawful immigration status, such as a visa or Lawful Permanent Resident status.

21. At approximately 1031 hours, after consulting with his wife by telephone, FIGUEROA also consented in writing to a search of his house and vehicles. ERO Deportation Officer Lonnie Hermann noticed that FIGUEROA mentioned a pistol in the house (in Spanish) when FIGUEROA was speaking to his wife by telephone. FIGUEROA also waived his Constitutional rights, both verbally and in writing, and agreed to answer questions if necessary.

22. Although FIGUEROA-Lopez was to wait at their residence for law enforcement to arrive, Shawnee, Kansas Police Officer Jake Morris observed her drive away and travel northbound. PO Morris (in his unmarked vehicle) assisted by following her to a business at 4005 Independence Avenue, Kansas City, Missouri, then back to her residence in Shawnee, Kansas.

23. S/A Sweetin and I contacted Frank ORDONEZ, the owner of Botanica, 4005 Independence Avenue Kansas City, Missouri, and he confirmed that FIGUEROA-Lopez had been there briefly, then left. S/A Sweetin and I, with assistance from Mr. Ordonez, attempted to locate any pistol that FIGUEROA-Lopez secreted in his business, but we were unable to locate a pistol or any other contraband or evidence.

24. S/A Sweetin and I met PO Morris near the house of FIGUEROA, but before we could contact FIGUEROA-Lopez, ERO Deportation Officer Kyle Ellis advised that FIGUEROA revoked his consent to search. This occurred at approximately 1205 hours. I have misplaced the original consent to search form, which was in Spanish, but have a photograph of it.

25. Due to the electronic evidence of violations of 18 U.S.C. § 1546(a), Visa Fraud, , S/A Sweetin and I detained the smartphone of FIGUEROA pending its possible seizure and search.

## TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings: Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless, device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of

calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

27. Based on my training, experience, and research, I know that cellular telephones have capabilities that allow it to serve as a wireless telephone, digital camera, and GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, and the location of the device's usage.

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. *Forensic evidence.* This application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the listed cellular telephones were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the listed cellular telephones because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, where the usage occurred, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, where it was used, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. Information stored within a cellular phone (cell phone) may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored within a cell phone can indicate who has used or controlled the cell phone. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, contacts lists, instant messaging logs, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the cell phone at a relevant time. Further, such stored electronic data can show how and when the cell phone and its related account were accessed or used. Such "timeline" information allows investigators to understand the chronological context of cell phone access, use, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the cell phone account owner. Additionally, information stored within a cell phone may indicate the geographic location of the cell phone and user at a particular time (e.g., location integrated into an image or video sent via email or text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the cell phone owner's state of mind as it relates to the offense under investigation. For example, information in the cell phone may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement). Unless this data is destroyed, by breaking the cell phone itself or by a program that deletes or over-writes the data contained within the cell phone, such data will remain stored within the cell phone indefinitely.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

31. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

*Manner of execution*.

a. Computer storage devices, (like modern day cellular phones, SIM cards and micro cards, hard disks, diskettes, tapes, laser disks, Bernoulli drives) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal

criminal evidence, and he or she might store criminal evidence in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crimes related to violations of Title 18 U.S.C. § 1546(a) and 922(g)(5). After the initial imaging, the examiner and agents will not further save or copy data unrelated to those violations. To the extent possible, they will minimize the review of unrelated data. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

b. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is good cause for the Court to authorize execution of the warrant at any time in the day or night.

## CONCLUSION

32. Based upon the foregoing, I believe there is probable cause that the listed digital device, and any incorporated SIM card and/or micro-SD card contain documents, photographs, text messages, direct messages, internet history, e-mails, "address books" or "contacts" lists, call logs, audio files, application data, and other types of electronic media, that constitutes evidence and/or fruits and instrumentalities of criminal offenses, including violations of 18 U.S.C. § 1546(a), Visa Fraud. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the digital device described in Attachment A, for the items listed in Attachment B.

EDGAR K JONES
Digitally signed by EDGAR K JONES
Date: 2024.11.04 08:28:17 -06'00'

Edgar Jones, Special Agent
Homeland Security Investigations

Subscribed to and sworn before me via reliable electronic means

on 4th day of November 2024. By telephone at 3:13 pm

HONORABLE W. BRIAN GADDY
United States Magistrate Judge
Western District of Missouri